

# Defining an Adaptive Software Security Metric from a Dynamic Software Fault-Tolerance Measure

Gary McGraw, Anup Ghosh, & Jeff Voas

Reliable Software Technologies Corporation

21515 Ridgetop Circle, Suite 250

Sterling, VA 20166

{gem,anup,jmvoas}@rstcorp.com      <http://www.rstcorp.com>

## Abstract

The original computer security defense strategy, circa 1970, was appropriately termed “penetrate and patch.” At that time, defense was entirely reactive — something that happened only after an attack was detected and some damage had already been inflicted. Penetrate and patch was followed by a series of more advanced defensive techniques (*e.g.*, real-time intrusion detection tools, COPS, and SATAN). Unfortunately, a recent proliferation of sophisticated threats has caused defensive security schemes to come full circle, back to where they began twenty-some years ago. Penetrate and patch has once again become the status quo.

This abstract briefly describes work-in-progress under ARPA contract number F30602-95-C-0282, “Quantifying Minimum-time-to-intrusion Based on Dynamic Software Safety Assessment”. We have developed a software metric that is currently being implemented to quantitatively assess information-system security and survivability. Our approach — called Adaptive Vulnerability Analysis (AVA) — exercises a piece of software (in source-code form) by simulating both malicious and non-malicious attacks that fall under various threat classes. AVA can be used to determine whether such threats undermine the security of the system. This approach stands in contrast to common security assurance methods that rely on black-box techniques for testing completely-installed software systems. AVA does not provide an *absolute* metric (such as mean-time-to-failure). However, it can be used as a relative metric, allowing a user to compare the security of different versions of a system, or to compare non-related systems with similar functionality.

AVA derives from models that were developed for assessing software fault-tolerance — in particular, a model used for Extended Propagation Analysis (EPA). Implemented models of EPA are automatic systems that use fault-injection methods to predict how software systems will behave when faced with anomalous circumstances such as: (1) simple and complex programmer errors, (2) rare but correct input data, (3) corrupted input data, and (4) failed hardware signals. In this ARPA-sponsored project, we are extending and adapting the functionality of EPA software-analysis models so that we will be able to predict the impact of an additional important class of anomalous circumstance on software systems — namely, malicious threats.

## References

- Voas, Jeff, Gary McGraw, & Anup Ghosh. Defining an Adaptive Software Security Metric from a Dynamic Software Failure Tolerance Measure. Reliable Software Technologies Technical Report. March 28, 1996. Sterling, VA.
- Voas, Jeff, Anup Ghosh, Gary McGraw, Frank Charron & Kieth Miller. (1996) Defining an adaptive software security metric from a dynamic software failure tolerance measure. In the *Proceedings of the Ninth Annual Conference on Computer Assurance*, pages 250-263. June 1996.